Cambridge OCR-set Assignment

Sample Assessment Material

Cambridge OCR Level 3 Alternative Academic Qualification
Cambridge Advanced National in Cyber Security and Networks

Unit F196: Digital forensic investigation

Scenario Title: Progress Insurance Company (PInC)

Valid for assessment from September 20XX to 20XX.
For use by students beginning the qualification in September 20XX.

This is a sample Cambridge OCR-set assignment which should only be used for practice.

This assignment **must not** be used for live assessment of students.

The live assignments will be available on our secure website, 'Teach Cambridge'.

The Cambridge OCR administrative codes linked to this unit are:

- unit entry code F196
- certification code H137

The regulated qualification number linked to this unit is:

610/6208/X

Duration

About 15 hours of supervised time (GLH)
(work that **must** be completed under teacher supervised conditions)

All this material **can** be photocopied. Any photocopying will be done under the terms of the Copyright Designs and Patents Act 1988 solely for

SAMPLE

the purposes of assessment.

SAMPLE

 © Cambridge OCR 2025

Contents

Information and instructions for teachers....3
Using this assignment....3
Information for delivering tasks....4
Tasks for students and assessment criteria....5
Scenario....5
Task 1....6
Task 2....8
Task 3....10
Teacher Observation Record Form....12
Guidance notes....13
NEA Command Words....14

SAMPLE

 © Cambridge OCR 2025

Information and instructions for teachers

Using this assignment

This assignment provides a scenario and set of related tasks that reflects how a digital forensic investigation could be completed.

You can give this to students on or after 1 June 202X to help them understand it before they start using it for assessment. The dates for which students can use it for assessment are shown on the front cover.

The assignment:
- Is written so that students have the opportunity to meet the requirements of all assessment criteria for the unit.
- Will tell students if their evidence must be in a specific format. If the task does not specify a format, students can choose the format to use.
- **Must** be completed under teacher supervision.

We have estimated that this assignment will take about 15 hours of supervised time to complete. Students should need approximately:
- 6 hours to complete Task 1.
- 5 hours to complete Task 2.
- 4 hours to complete Task 3.

You **must**:
- Use a Cambridge OCR-set assignment for summative assessment of students.
- Familiarise yourself with the assessment criteria and assessment guidance for the tasks. These are given at the end of each student task. They are also with the unit content in **Section 5** of the Specification.
  Assessment guidance is only given where additional information is needed. There might not be assessment guidance for each criterion.
- Make sure students understand that the assessment criteria and assessment guidance tell them in detail what to do in each task.
- Read and understand **all** the rules and guidance in **Section 7** of the Specification **before** your students start the set assignments.
- Make sure that your students complete the tasks and that you assess the tasks fully in line with the rules and guidance in **Section 7** of the Specification.
- Give your students the **Cyber Security and Networks Student guide to NEA assignments before** they start the assignments.
- Complete the **Teacher Observation Record** for **Task 2**. You **must** follow the guidance given when completing it.

You **must not**:

© Cambridge OCR 2025

- Use live Cambridge OCR-set assignments for practice or formative assessment. This sample assessment material **can** be used for practice or formative assessment.
- Use this sample assessment material for live assessment of students.
- Allow group work for **any** task in this assignment.
- Change any part of the Cambridge OCR-set assignments or assessment criteria.

Information for delivering tasks

Task	Requirements
Task 2	• A forensic image (forensic copy) of the physical storage device described in the scenario **must** be downloaded by the centre and made available to students to use in their digital forensic investigation. • Students **must** use digital forensic tools, techniques and working methods to examine the image and gather evidence as required by the task

Sample set assignment - forensic image notes: (not disclosed on live assignments)

A forensic image (forensic copy) of a desktop hard disk drive which accompanies the scenario will be supplied for students to use in their investigation.

For this sample set assignment, the image will include:

- Windows 10 build with file system intact.
- Connected to the PInC domain and accounts created for generic user.
- Second user account (hidden) created locally, deleted.
- Documents on main account desktop, with company/customer data. Delete as main user.
- Zip in hacker's folder with weak password of files taken from main desktop.
- HTML document replicating a spreadsheet with input boxes for username and passwords stating "enter login details to access file" – this will have a URL made up where the details are forwarded to - P1nc.org rather than PInC.org.
- The spreadsheet will state an update will be required which will install the backdoor
- Reverse shell traffic can be tested and recorded with Wireshark from the sandbox environment.
- Browser history.

SAMPLE

 © Cambridge OCR 2025

Pages 1-4 are for teachers only. Please do **not** give **Pages 1-4** to your students.

You can give **any** or **all** of the pages **that follow** to your students.

SAMPLE

 © Cambridge OCR 2025

Tasks for students and assessment criteria

Unit F196: Digital forensic investigation

Scenario title: Progress Insurance Company (PInC)

Valid for assessment from September 20XX to 20XX.
For use by students beginning the qualification in September 20XX.

Scenario

Progress Insurance Company (PInC) provides different types of insurance to customers including car and home insurance. Customers need to register online to be able to access their policy documents. PInC stores personal data from their customers to be able to offer the best price. This data is stored in a Management Information System which has tiered access via a web portal by staff.

PInC has been made aware that there is a possibility that they have suffered a data breach through a phishing attack. An anonymous source contacted the company with information taken from a forum on the dark web. The dark web is used by hackers to post their recent activities. The source said that an employee fell for a phishing attack and ran malware allowing the attacker to access sensitive information.

An0n wrote:

“I had a hit from a phishing trip last week. The employee works at Progress Insurance Company. They downloaded a fake spreadsheet with information on proposed staff pay cuts, and then used their account details to “log in” to the fake spreadsheet. I got access to their emails and the employee installed a “plugin” so they could read the fake spreadsheet. It gave me full access to their computer… they probably shouldn’t have kept all their customers’ information on their desktop.”

After learning which employee and device were affected, the Chief Information Security Officer has asked you to plan and complete an investigation into the incident. You need to gather enough evidence to confirm the system was breached, and whether any data and information has been affected. PInC is also concerned that some data has either been deleted, transformed and/or hidden.

SAMPLE

 © Cambridge OCR 2025

Task 1
Planning the digital forensic investigation

Topic Areas 1, 2 and 3 are assessed in this task

The task is:

Plan the digital forensic investigation for Progress Insurance Company (PInC).

Your evidence **must** include:

- A digital forensic investigation plan.
- Written evidence.

Use the assessment criteria below to tell you what you need to do in more detail.

Pass	Merit	Distinction
P1: Identify the aim, scope and scene of the digital forensic investigation. (PO2)		
P2: Describe the digital evidence required and possible sources for the digital forensic investigation. (PO2)		
P3: Describe the tools and techniques to be used to handle evidence in the digital forensic investigation. (PO2)	**M1: Justify** the choice of tools and techniques planned to collect and secure evidence during the digital forensic investigation. (PO3)	**D1: Discuss** the implications of different factors of digital forensics when completing the digital forensic investigation. (PO3)
	M2: Explain how the evidence in the digital forensic investigation will be preserved. (PO2)	
P4: Identify potential issues for the digital forensic investigation. (PO2)	**M3: Explain** the legal and ethical considerations which will impact the digital forensic investigation. (PO2)	**D2: Discuss** how digital forensic challenges will impact the digital forensic investigation. (PO3)

SAMPLE

© Cambridge OCR 2025

Assessment Guidance

This assessment guidance gives you information to meet the assessment criteria. There might not be additional assessment guidance for each criterion. It is only given where it is needed. You must read this guidance before you complete your evidence.

Assessment Criteria	Assessment guidance
P1	• Students **must** use the information given in the scenario to identify the aim, scope and scene of the digital forensic investigation. Any assumptions **must** be stated. This assessment criterion **must** be evidenced in the digital forensic investigation plan.
P2	• Students **must** describe what evidence they are looking for during the investigation and where they could find it. Any assumptions **must** be stated. This assessment criterion **must** be evidenced in the digital forensic investigation plan.
P3	• Students **must** describe which tools and techniques they are going to use to complete their digital forensic investigation. The tools and techniques selected **must** be appropriate for the investigation they intend to complete. This assessment criterion **must** be evidenced in the digital forensic investigation plan.
P4	• This assessment criterion **must** be evidenced in the digital forensic investigation plan.
M1	• M1 builds on P3. Students **must** justify their choice of tools and techniques they intend to use. The justifications **must** link to the actual investigation students intend to complete. This assessment criterion **must** be evidenced in the digital forensic investigation plan.
M2	• Students' explanations **must** link to the actual investigation students intend to complete. This assessment criterion **must** be evidenced in the digital forensic investigation plan.
M3	• Students **must** explain how the legal and ethical considerations in Topic Area 1.2 impact their investigation. Legal and ethical considerations which are not included in Topic Area 1.2 **could** also be explained.
D1	• Students **must** discuss how the factors in Topic Area 1.1 implicate their investigation.
D2	• Students **must** use content in Topic Area 1.2.3 in their discussions.

SAMPLE

 © Cambridge OCR 2025

Task 2
Completing the digital forensic investigation

Topic Areas 2, 3 and 5 are assessed in this task

The task is:

Complete the digital forensic investigation planned in **Task 1**.

- You will use digital forensic tools and techniques to complete the planned digital forensic investigation.
- You will also check the evidence found meets the needs of the digital forensic investigation.

Your evidence **must** include:

- Photos, videos and other evidence of completing the digital forensic investigation.
- A teacher observation record form signed by you and your teacher.
- Recorded outcomes.
- Written evidence.

Use the assessment criteria below to tell you what you need to do in more detail.

<table>
<tr><th>Pass</th><th>Merit</th><th>Distinction</th></tr>
<tr><td>P5: Use tools and techniques to collect digital forensic evidence. (PO4)</td><td rowspan="3">M4: Explain how the principles of data storage have been used to collect, recover and preserve the digital forensic evidence. (PO2)</td><td rowspan="3">D3: Assess the suitability of the tools and techniques used to collect, recover and preserve digital forensic evidence.
(PO3)</td></tr>
<tr><td>P6: Use tools and techniques to recover digital forensic evidence. (PO4)</td></tr>
<tr><td>P7: Use tools and techniques to preserve digital forensic evidence. (PO4)</td></tr>
<tr><td>P8: Use tools and techniques to confirm the integrity and accuracy of the digital forensic evidence. (PO4)</td><td rowspan="2">M5: Discuss how the evidence found meets the needs of the digital forensic investigation. (PO3)</td><td rowspan="2"></td></tr>
<tr><td>P9: Record the outcomes of the digital forensic investigation in an appropriate format. (PO4)</td></tr>
</table>

SAMPLE

© Cambridge OCR 2025

Assessment Guidance

This assessment guidance gives you information to meet the assessment criteria. There might not be additional assessment guidance for each criterion. It is only given where it is needed. You must read this guidance before you complete your evidence.

<table>
<tr><th>Assessment Criteria</th><th>Assessment guidance</th></tr>
<tr><td colspan="2">During this task students must collect and preserve all the evidence detailed in their digital forensic investigation plan. Students could also collect and preserve other evidence not on their initial plan depending on how the investigation progresses - they must not be penalised for doing this.</td></tr>
<tr><td>P5
P6
P7
P8</td><td>• Students must start off their investigation by using the tools and techniques planned in Task 1, to collect digital evidence. Students could deviate from their plan if they find other tools and techniques are needed.
• An individualised teacher observation record (TOR) form must be provided for each student as evidence of the digital forensic tools and techniques used to complete the planned digital forensic investigation (Task 2, Topic Area 3). Students must also read and sign the TOR form. Each TOR form must describe the digital forensic tools and techniques used by the student. For this task students must also provide evidence such as photos or videos showing them collecting digital evidence during their digital forensic investigation.</td></tr>
<tr><td>P9</td><td>• Students must record the evidence found in one of the formats listed in Topic Area 3.3.</td></tr>
<tr><td>M4</td><td>• Students must explain how they have used the principles in Topic Area 3.1 during their collection, recovery, and preservation of digital evidence.</td></tr>
<tr><td>M5</td><td>• Students must relate their discussion back to the digital forensic investigation plan written in Task 1. Where students have deviated from the evidence requirements planned, they must justify why.</td></tr>
<tr><td>D3</td><td>• Students must assess the suitability each tool and technique used during the collection, recovery and preservation of digital evidence. The assessment must be based on how successful the tools and techniques were – did they find anything? if nothing was found, why did it fail? Where students have deviated from the tools and techniques planned, in task 1, they must justify why.</td></tr>
</table>

SAMPLE

 © Cambridge OCR 2025

Task 3
Reporting findings and reviewing the digital forensic investigation

Topic Areas 4 and 5 are assessed in this task

The task is:

Create a report of the digital forensic investigation findings from **Task 2**.

- You will need to create a report of the digital forensic investigation for the Chief Information Security Officer of PInC.

Review the plan from **Task 1** and processes followed to complete the digital forensic investigation in **Task 2**.

Your evidence **must** include:

- A report of the digital forensic investigation findings.
- Written evidence.

Use the assessment criteria below to tell you what you need to do in more detail.

Pass	Merit	Distinction
P10: Create a report of the digital forensic investigation findings. (PO4)	**M6: Justify** the conclusions made in the digital forensic investigation findings report. (PO3)	**D4: Discuss** the accuracy, reliability, and repeatability of the digital forensic investigation. (PO3)
P11: Explain how the presentation of the digital forensic investigation findings report is suitable for the intended audience. (PO2)		
P12: Assess the effectiveness of the digital forensic investigation plan. (PO3)	**M7: Discuss** how the quality of the investigation has been impacted by constraints. (PO3)	**D5: Justify** potential improvements to the digital forensic investigation. (PO3)

SAMPLE

 © Cambridge OCR 2025

Assessment Guidance

This assessment guidance gives you information to meet the assessment criteria. There might not be additional assessment guidance for each criterion. It is only given where it is needed. You must read this guidance before you complete your evidence.

Assessment Criteria	Assessment guidance
P10	• Students **must** create a report which shows the findings of their digital forensic investigation. It should follow the report structure given in Topic Area 4.1. This assessment criterion is not looking for detailed explanations or justifications in each report section but for the content to be communicated appropriately for the intended audience.
P11	• Students **must** explain how they have adapted the report presentation considerations listed in Topic Area 4.1 to suit the intended audience for their digital forensic investigation report.
P12	• Students **must** assess how successful their digital forensic investigation plan created in Task 1 was. Students **must** explain which aspects of the investigation were fully planned and which were not.
M6	• Students **must** justify why they have come to the investigation conclusion, based on the evidence found.
M7	• Students **must** discuss how their digital forensic investigation has been both positively and negatively impacted by constraints. Topic Area 5.2 contains types of constraint which students **must** consider.
D4	• Students **must** discuss the accuracy of what they did in Task 2 and what they found out. • Students **must** also discuss if the investigation was to be completed again, perhaps using different methods, would the same conclusion be reached.
D5	• Students **must** justify what they would do differently next time and why.

SAMPLE

 © Cambridge OCR 2025

Teacher Observation Record Form

Use this form to record what is observed.
Read the **guidance notes** below the form **before** you complete the form.

Cambridge OCR Level 3 Alternative Academic Qualification Cambridge Advanced National in Cyber Security and Networks (Extended Certificate)

Unit number:	F196
Unit title:	Digital forensic investigation
Task number:	2
Task title:	Completing the digital forensic investigation

Student's name:	
Date the activity was completed:	

What extra evidence is attached to the form?	

The **teacher** fills in this section:

What Assessment Criteria does this activity relate to? **P5:** Use tools and techniques to collect digital forensic evidence. **P6:** Use tools and techniques to recover digital forensic evidence. **P7:** Use tools and techniques to preserve digital forensic evidence. **P8:** Use tools and techniques to confirm the integrity and accuracy of the digital forensic evidence.
How does the activity meet the requirements of the Assessment Criteria? You **must** describe: 1. What the student did 2. How it relates to the relevant Assessment Criteria

Teacher's name:	
Teacher's signature:	
Date:	

SAMPLE

© Cambridge OCR 2025

The **student** fills in this section:

I agree with my teacher's description of how I completed this activity Yes ☐	
Use this space to make any extra comments.	
Student's signature:	
Date:	

Guidance notes

Both the teacher **and** the student are responsible for completing this form.

The **teacher must**:
- use the form to describe in detail what they observed the student doing.
- give contextualised details of what the student did and how this relates to the Assessment Criteria.
- say how well the activity was completed in relation to the Assessment Criteria with reasons.
- share what they have written with the student and offer the opportunity to discuss if the student disagrees with what is written.
- reach agreement with the student before the work is submitted for moderation.
- sign and date the form as evidence of agreement.

The **student must**:
- reach agreement with the teacher before the work is submitted for moderation.
- use the form to show that they agree with the teacher's record of the activity observed.
- sign and date the form as evidence of agreement.

The form **must**:
- be accompanied by extra evidence, as required by the task.
- provide evidence that is individual to the student.

The form **must not**:
- contain a simple repeat of the Assessment Criteria.
- contain just a list of skills.
- be completed by anyone other than the teacher observing the activity and the student completing the activity.
- be written by the student for the teacher to sign.
- be used to evidence achievement of a whole unit or task in isolation.

SAMPLE

© Cambridge OCR 2025

SAMPLE

 © Cambridge OCR 2025

NEA Command Words

The table below shows the command words that may be used in the NEA assignments and/or assessment criteria.

Command Word	Meaning
Adapt	• Change to make suitable for a new use or purpose
Analyse	• Separate or break down information into parts and identify their characteristics or elements • Explain the different elements of a topic or argument and make reasoned comments • Explain the impacts of actions using a logical chain of reasoning
Assess	• Offer a reasoned judgement of the standard or quality of situations or skills. The reasoned judgement is informed by relevant facts
Calculate	• Work out the numerical value. Show your working unless otherwise stated
Classify	• Arrange in categories according to shared qualities or characteristics
Compare	• Give an account of the similarities and differences between two or more items, situations or actions
Conclude	• Judge or decide something
Describe	• Give an account that includes the relevant characteristics, qualities or events
Discuss (how/whether/etc)	• Present, analyse and evaluate relevant points (for example, for/against an argument) to make a reasoned judgement
Evaluate	• Make a reasoned qualitative judgement considering different factors and using available knowledge/experience
Examine	• To look at, inspect, or scrutinise carefully, or in detail
Explain	• Give reasons for and/or causes of something • Make something clear by describing and/or giving information
Interpret	• Translate information into recognisable form • Convey one's understanding to others, e.g. in a performance
Investigate	• Inquire into (a situation or problem)
Justify	• Give valid reasons for offering an opinion or reaching a conclusion
Research	• Do detailed study in order to discover (new) information or reach a (new) understanding
Summarise	• Express the most important facts or ideas about something in a short and clear form

We might also use other command words but these will be:

SAMPLE

© Cambridge OCR 2025

- commonly used words whose meaning will be made clear from the context in which they are used.
- subject specific words drawn from the unit content.

SAMPLE

 © Cambridge OCR 2025